

1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI
(c) 2005 Thomson Derwent. All rts. reserv.



013461376 **Image available**
WPI Acc No: 2000-633319/ 200061
XRPX Acc No: N00-469338

Security system has IC card reader-writer to rewrite valid access information in access key of user to invalid access information when operating system is not operated within preset time after permitting access

Patent Assignee: HITACHI COMPUTER ELECTRONICS KK (HITA-N)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2000259277	A	20000922	JP 9964966	A	19990311	200061 B

Priority Applications (No Type Date): JP 9964966 A 19990311

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 2000259277	A	9	G06F-001/00	

Abstract (Basic): JP 2000259277 A

NOVELTY - Each authenticated user has access key to store user validity details for accessing operating system (206) of computer (103). User's access key is read and validated by IC card reader-writer to permit access to operating system. When user does not operate operating system within preset time, his access right is prohibited and IC card reader-writer rewrites information in access key to be invalid.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for security procedure.

USE - In computer system for authentication of user.

ADVANTAGE - Since the IC card reader-writer rewrites validity to access information stored in access key as invalidity to access, access of system by third person is eliminated.

DESCRIPTION OF DRAWING(S) - The figure shows the software configuration of electronic computer system.

Computer (103)

Operating system (206)

pp; 9 DwgNo 2/5

Title Terms: SECURE; SYSTEM; IC; CARD; READ; WRITING; REWRITING; VALID; ACCESS; INFORMATION; ACCESS; KEY; USER; INVALID; ACCESS; INFORMATION; OPERATE; SYSTEM; OPERATE; PRESET; TIME; AFTER; PERMIT; ACCESS

Derwent Class: T01

International Patent Class (Main): G06F-001/00

International Patent Class (Additional): G06F-015/00

File Segment: EPI

(11)特許出願公開番号
特開2000-259277
(P2000-259277A)

(43)公開日 平成12年9月22日(2000.9.22)

(51)Int.Cl. ⁷		識別記号	F I	データベース ^(参考)	
G 0 6 F	1/00	3 7 0	G 0 6 F	1/00	3 7 0 E 5 B 0 8 5
	15/00	3 3 0		15/00	3 3 0 G

審査請求 未請求 請求項の数6 O.L (全 9 頁)

(21)出願番号 特願平11-64966

(22)出願日 平成11年3月11日(1999.3.11)

(71)出願人 000153454

株式会社日立インフォメーションテクノロジー

神奈川県足柄上郡中井町境456番地

(72) 発明者 中道 聡

神奈川県秦野市堀山下1番地 株式会社日立インフォメーションテクノロジー内

(72) 発明者 春山 和博

神奈川県秦野市堀山下1番地 株式会社日
立インフォメーションテクノロジー内

(74) 代理人 100087170

弁理士 富田 和子

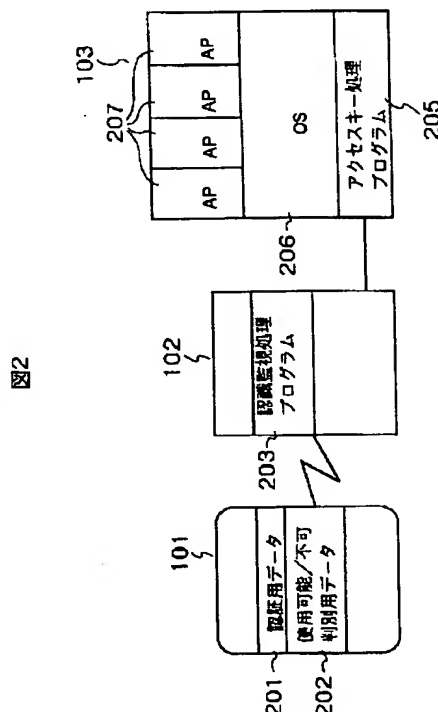
Fターム(参考) 5B085 AE12 AE13

(54) 【発明の名称】 セキュリティシステムおよびセキュリティ方法

(57) 【要約】

【課題】 アクセスキーをシステムに接続したまま放置された場合に、第三者によるシステムへの不正なアクセスを排除する。

【解決手段】電子計算機１０３のアクセスキー処理プログラム２０５は、使用可能／不可判別用データ２０２に使用可能を表すデータが書き込まれた正当なアクセスキー１０１がＩＣカードリーダライタ１０２に接続されると、ＯＳ２０６を動作させ、利用者にシステムへのアクセスを認めるが、その後、一定時間以上、利用者よりの入力が無かった場合には、アクセスキー１０１が放置されたものと見なして、ＯＳ２０６を停止させ、かつ、アクセスキー１０１の使用可能／不可判別用データ２０２を使用不可を表すデータに書き換えＯＳ２０６を動作させることができないようにすることにより、他者のシステムへの不正なアクセスを排除する。



【特許請求の範囲】

【請求項 1】保護対象システムへのアクセスを許可する利用者を限定するセキュリティシステムであって、利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーに対して読み書きを行うアクセスキー読み書き手段と、

前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するアクセス許可手段と、利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるアクセスキー無効化手段とを有することを特徴とするセキュリティシステム。

【請求項 2】請求項 1 記載のセキュリティシステムであって、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが無効である旨を示す場合に、利用者より、利用者を認証可能な情報の入力を受け付け、受け付けた情報から、前記保護対象システムへのアクセスを許可する利用者を認証できた場合に、利用者の前記保護対象システムへのアクセスを許可すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが有効である旨を示す使用可否データに書き換えるアクセスキー有効化手段を有することを特徴とするセキュリティシステム。

【請求項 3】保護対象システムへのアクセスを許可する利用者を限定するセキュリティ方法であって、利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可し、利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキー

の使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えることを特徴とするセキュリティ方法。

【請求項 4】電子計算機に読み取られ実行されるプログラムを記憶した記憶媒体であって、前記プログラムは、前記電子計算機に、利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するステップと、利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるステップとを実行させることを特徴とする記憶媒体。

【請求項 5】保護対象システムへのアクセスを許可する利用者を限定するセキュリティシステムであって、利用者を認証するための認証用データを記憶したアクセスキーに対して読み書きを行うアクセスキー読み書き手段と、各アクセスキーの有効／無効を表す使用可否データを記憶する使用可否データ記憶手段と、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記使用可否データ記憶手段に記憶された前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するアクセス許可手段と、利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記前記使用可否データ記憶手段に記憶された使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるアクセスキー無効化手段とを有することを特徴とするセキュリティシステム。

【請求項 6】請求項 1、2 または 5 記載のセキュリティシステムと、前記保護対象システムとを有し、前記保護対象システムは、電子計算機上で稼働するシステムであることを特徴とする電子計算機システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、システムへのアク

セスを許可する利用者の認証にアクセスキーを用いる技術に関するものである。

【0002】

【従来の技術】電子計算機上に構築されるシステムのセキュリティを高めるためにシステムへのアクセスを特定の利用者に限定する技術として、アクセスキーを利用者の認証に用いる次のような技術が知られている。

【0003】すなわち、この技術では、あらかじめ、システム（OSや特定のアプリケーション）へのアクセスを認める特定の利用者に、認証用の情報を記憶させたICカードをアクセスキーとして配布する。そして、アクセスキーを配布された利用者は、システム利用開示に、このアクセスキーをシステムに電氣的または電磁氣的に接続し読み取らせる。システムは読み取ったアクセスキーに記憶された認証用の情報が正規のものであれば、利用者にシステムへのアクセスを許可する。

【0004】そして、システムへのアクセスを許可した後、引き続きアクセスキーを監視し、正規の認証用の情報が記憶されているアクセスキーを認識できなくなると、再度、正規の認証用の情報が記憶されているアクセスキーを認識できるまで、システムを停止する。

【0005】このようなアクセスキーを利用者の認証に用いる技術によれば、利用者は、自分がシステムへアクセスする権限を有することをシステムに示すために、認証用の情報（たとえば個人IDやパスワードなど）をキーボードなどから、システム利用の度にいちいち入力する必要がなくなる。また、システム利用途中で、システムを離れる場合も、アクセスキーを共に持ち去れば、この間に第三者が不正にシステムにアクセスすることを排除することができる。

【0006】

【発明が解決しようとする課題】前記従来のアクセスキーを利用者の認証に用いる技術によれば、システム利用途中でアクセスキーをシステムに接続したまま、利用者がシステムを離れてしまった場合には、この間に第三者が、このアクセスキーを用いて不正にシステムにアクセスすることが可能となる。また、そのまま第三者にアクセスキーを持ち去られてしまった場合には、その後、このアクセスキーを用いた第三者によってシステムに不正にアクセスされてしまう可能性がある。

【0007】そこで、本発明は、システム利用途中でアクセスキーをシステムに接続したまま、利用者がシステムを離れてしまった場合に、第三者による、システムへの不正なアクセスを排除することを課題とする。

【0008】

【課題を解決するための手段】前記課題達成のために、本発明は、たとえば、保護対象システムへのアクセスを許可する利用者を限定するセキュリティシステムであって、利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したア

クセスキーに対して読み書きを行うアクセスキー読み書き手段と、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するアクセス許可手段と、利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるアクセスキー無効化手段とを有することを特徴とするセキュリティシステムを提供する。

【0009】このようなセキュリティシステムによれば、正当なアクセスキーが提示されると、利用者に保護対象システムへのアクセスを許可するが、その後、一定時間以上、利用者よりの何の入力も無かった場合には、アクセスキーの正当な所持者がアクセスキーを放置したものと見なして、保護対象システムへのアクセスを禁止し、かつ、アクセスキーの使用可否データを無効を表すデータに書き換え、このアクセスキーによって保護対象システムへのアクセスが許可されないようにすることにより、他者の不正なアクセスを排除することができる。

【0010】

【発明の実施の形態】以下、本発明の実施形態を説明する。

【0011】図1に本実施形態に係る電子計算機システムの構成を示す。

【0012】図示するように、本実施形態に係る電子計算機システムは、電子計算機（以下、「PC」と記す）103と、ICカードを用いたアクセスキー101の読み書きを行うICカードリーダライタ102より構成される。

【0013】ICカードリーダライタ102は、PC103と接続されており、PC103から制御することができる。

【0014】次に、本電子計算機システムのソフトウェア構成を図2に示す。

【0015】図示するように、PC103は、アクセスキー処理プログラム205、OS206、OS206上で稼働するアプリケーションプログラム207が組み込まれている。ただし、アクセスキー処理プログラム205はOS206の一部として、OS206に組み込まれるものであってもよい。また、ICカードリーダライタ102は、ICカードリーダライタ102内部に備えられたプロセッサで実行される認識監視処理プログラム2

5

03が組み込まれている。また、アクセスキー101には、認証用データ201と使用可能／不可判別用データ202が記憶される。

【0016】なお、PC103のハードウェア構成は、図3に示すように、CPU301、主記憶302、入力装置303、表示装置304、外部記憶装置305、306、外部入出力インタフェース308などを備えた一般的な電子計算機の構成を有する。

【0017】このようなハードウェア構成において、アクセスキー処理プログラム205、OS206、アプリケーションプログラム207の各プログラムは、外部記憶装置305、306に記憶されており、CPU301は、外部記憶装置305、306に記憶されたこれらプログラムを主記憶302にロードし実行する。なお、これらのアクセスキー処理プログラム205、OS206、アプリケーションプログラム207は、外部記憶装置306にマウントされたリムーバブルな記憶媒体307から、直接、もしくは、一旦、他の外部記憶装置305に記憶された後、主記憶302にロードされるものであってよい。

【0018】以下、このような電子計算機システムの動作について説明する。

【0019】まず、ICカードリーダライタ102の認識監視処理プログラム203の動作について説明する。

【0020】図4に、認識監視処理プログラム203の動作の手順を示す。

【0021】図示するように、ICカードリーダライタ102が起動されると、認識監視処理プログラム203は起動され、PC103からの命令待ちの状態となる。そして、PC103からアクセスキー101の認識監視の開始命令を受け付けると（ステップ401）、まず、アクセスキー101の認証用データ201と使用可能／不可判別用データ202を電氣的または電磁氣的に読み出し（ステップ402）、これらを読み込んだ場合には（ステップ403）、これまで同データを記憶したアクセスキー101を認識していたか否かを調べる（ステップ406）。ここでは、具体的には、前回行ったステップ402で認証用データ201と使用可能／不可判別用データ202が読み出されており、かつ、今回行ったステップ402で読み出した認証用データ201と使用可能／不可判別用データ202が前回行ったステップ402で読み出した認証用データ201と使用可能／不可判別用データ202と同じである場合には、これまで同データを記憶したアクセスキー101を認識していたと判定し、他の場合には、これまで同データを記憶したアクセスキー101を認識していなかったと判定する。但し、今回行ったステップ402が起動後最初に行われたステップ402である場合には、これまで同データを記憶したアクセスキー101を認識していなかったと判定する。

6

【0022】そして、ステップ406で、これまで同データを記憶したアクセスキー101を認識していたと判定された場合には、ステップ411に進む。

【0023】一方、ステップ406で、読み出した使用可能／不可判別用データ202が使用可能を表しているかどうかを判定し（ステップ408）、使用可能を表していると判定された場合には、PC103へ使用可能のアクセスキー101を認識した事を今回行ったステップ402で読み出した認証用データ201と共に報告し（ステップ410）、使用不可を表していると判定された場合には、PC103へ使用不可のアクセスキー101を認識した事を今回行ったステップ402で読み出した認証用データ201と共に報告する（ステップ409）。そして、ステップ411に進む。

【0024】この結果、ICカードリーダライタ102に使用可能／不可判別用データ202が使用可能を表しているアクセスキー101が電氣的又は電磁氣的に接続されると、その時点（ICカードリーダライタ102の起動前に既に接続されている場合には起動時）で、PC103へ使用可能のアクセスキー101を認識した事がアクセスキー101に記憶された認証用データ201と共に報告される。また、ICカードリーダライタ102に使用可能／不可判別用データ202が使用不可を表しているアクセスキー101が接続されると、その時点（ICカードリーダライタ102の起動前に既に接続されている場合には起動時）で、PC103へ使用不可のアクセスキー101を認識した事がアクセスキー101に記憶された認証用データ201と共に報告される。

【0025】また、さらに、ICカードリーダライタ102に接続されたアクセスキー101の使用可能／不可判別用データ202が書き換えられると、使用可能を表すデータに書き換えられた場合にはPC103へ使用可能のアクセスキー101を認識した事がアクセスキー101に記憶された認証用データ201と共に報告され、使用不可を表すデータに書き換えられた場合にはPC103へ使用不可のアクセスキー101を認識した事がアクセスキー101に記憶された認証用データ201と共に報告される。

【0026】さて、ステップ411では、PC103から使用可能／不可判別用データ202の書き換え命令を受けたかどうかを調べ、受けている場合には、書き換え命令に従ってアクセスキー101の使用可能／不可判別用データ202を書き換え（ステップ412）、ステップ413に進む。一方、書き換え命令を受けていない場合には、そのままステップ413に進む。

【0027】一方、先のステップ403においてアクセスキー101の認証用データ201と使用可能／不可判別用データ202を読み出すことができなかった場合には、ステップ404において、これまでアクセスキー101を認識していたかどうかを調べる。ここでは、具体

的には、前回行ったステップ402でアクセスキー101の認証用データ201と使用可能／不可判別用データ202を読み出すことができている場合には、これまでアクセスキー101を認識していたと判定し、他の場合は、これまでアクセスキー101を認識していなかったと判定する。ただし、今回行ったステップ402が起動後最初に行われたステップ402である場合には、これまでアクセスキー101を認識していなかったと判定する。そして、これまでアクセスキー101を認識していなかったと判定された場合には、ステップ413に移行し、これまでアクセスキー101を認識していたと判定された場合には、PC103にアクセスキー101が認識できなくなったことを報告し（ステップ405）、ステップ413に進む。結果、ICカードリーダーライタ102からアクセスキー101が取り外されると、PC103にアクセスキー101が認識できなくなったことが報告される。

【0028】最後に、ステップ413では、PC103から終了命令を受けたかどうかを調べ、受けている場合には、ステップ401に、受けていない場合にはステップ402に戻る。

【0029】次に、PC103のアクセスキー処理プログラム205の動作について説明する。

【0030】図5に、アクセスキー処理プログラム205の動作手順を示す。

【0031】図示するようにPC103が起動されると、アクセスキー処理プログラム205が起動される。起動されたアクセスキー処理プログラム205は、ICカードリーダーライタ102にアクセスキー101の認識監視の開始命令を送信する（ステップ500）。そして、最後にICカードリーダーライタ102から受け取った報告が使用可能もしくは使用不可のアクセスキー101を認識したことの報告となるまで待つ（ステップ501）。なお、ここで、まだ何の報告も受け取っていない場合には、これら報告を受信することにより最後にICカードリーダーライタ102から受け取った報告が使用可能もしくは使用不可のアクセスキー101を認識したことの報告となる。そして、最後にICカードリーダーライタ102から受け取った報告が使用可能もしくは使用不可のアクセスキー101を認識したことの報告となつたならば、報告と共に受け取った認証用データ201を、あらかじめアクセスキー処理プログラム205に登録された認証データと比較することにより検証し（ステップ502）、正当なものでなければステップ501に戻り、正当なものであればステップ503に進む。

【0032】ステップ503では、この最後に受け取った報告が使用可能のアクセスキー101を認識したことの報告であるかどうかを判定し（ステップ503）、そうであれば、OS206を起動、動作させる（ステップ507）。これにより、利用者はPC103を利用可能

となる。

【0033】さて、ステップ507で、OS206を起動、動作させた後は、ユーザーからのキー入力、マウス入力などの各種入力を監視し、一定時間内に何らかの入力が利用者よりなされたかどうかを調べ（ステップ508）、一定時間内に入力がなかった場合は、ICカードリーダーライタ102に、アクセスキー101の使用可能／不可判別用データ202を使用不可を表すデータに書き換える使用可能／不可判別用データ202の書き換え命令を送信し（ステップ509）、OS206の動作を停止させ（ステップ511）、ステップ501に戻る。

【0034】一方、一定時間内に入力があつた場合は、同データを記憶したアクセスキー101を認識中かどうかを判定する（ステップ510）。ここでは、具体的には、先にステップ501の判定で最後の報告として取り扱った報告以降、何の報告もICカードリーダーライタ102から受け取っていない場合には、同データを記憶したアクセスキー101を認識中であると判定し、他の場合には、同データを記憶したアクセスキー101を認識中でないと判定する。そして、同データを記憶したアクセスキー101を認識中でないと判定された場合には、OS206の動作を停止させ（ステップ511）、ステップ502に戻る。

【0035】一方、同データを記憶したアクセスキー101を認識中である場合には、利用者よりOS206の終了を指示されているかどうかを調べ、指示されていない場合には、ステップ508に戻り、指示されている場合には、OS206を終了させ、ICカードリーダーライタ102に終了命令を発行し、処理を終了する。

【0036】一方、先のステップ503において、最後の報告が使用不可のアクセスキー101を認識したことの報告であると判定された場合には、利用者に認証用データを入力させ（ステップ504）、入力された認証用データが正当なものであるかどうかを当該入力されたデータをあらかじめアクセスキー処理プログラム205に登録された認証データと比較することにより調べ（ステップ505）、入力された認証用データが正当なものであれば、ICカードリーダーライタ102に、アクセスキー101の使用可能／不可判別用データ202を使用可能を表すデータに書き換える使用可能／不可判別用データ202の書き換え命令を送信し（ステップ506）、ステップ507に進んでOS206を起動、動作させる。一方、入力された認証用データが正当なものでなければステップ501に戻る。

【0037】以上のような本実施形態に係る電子計算機システムの動作によれば、正当なアクセスキー101がICカードリーダーライタ102に接続されると、OS206を動作させ、利用者がアクセス可能とするが、その後、一定時間以上、利用者よりの入力が無かつた場合には、アクセスキー101の正当な所持者がアクセスキー

101を放置したものと見なして、OS206を停止させ、かつ、アクセスキー101の使用可能／不可判別用データ202を使用不可を表すデータに書き換えOS206を動作させることができないようにすることにより、他者の不正なアクセスを排除することができる。

【0038】一方、このように使用不可にしたアクセスキー101が正当な所持者の手によって使用される場合には、再度、このアクセスキー101によってOS206を動作させアクセスすることが可能となるように、正当な所持者の認証用データの入力によってアクセスキー101の使用可能／不可判別用データ202を使用可能を表すデータに書き換える。したがって、正当な所持者がアクセスキー101を放置せず、熟慮や居眠りなどにより、一定時間以上入力しなかったために、OS206が停止し、アクセスキー101が使用できなくなった場合にも、正当な利用者であれば、即座に、OSを再動作させ、アクセスキーを使用可能とすることができる。

【0039】以上、本発明の実施形態について説明した。

【0040】なお、以上の実施形態において、ICカードリーダライタ102において、PC103の電源を監視し、PC103の電源OFF後、一定時間以上、アクセスキー101を認識し続けた場合には、アクセスキー101の使用可能／不可判別用データ202を使用不可を表すデータに書き換えるようにしてもよい。

【0041】また、以上の実施形態では、アクセスキー101によりアクセスを可能とする対象を全アプリケーションプログラム207を含むOS206上で実現される全機能としたが、これは、個々のアプリケーションプログラム207とするようにしてもよい。

【0042】また、本実施形態に係るアクセスキーの技術は、電子計算機システムに限らず、任意の装置、システムに適用可能である。

【0043】また、アクセスキーとしては、ICカードの他、メモリカードや、その他の各種記録媒体を用いるようにしてもよい。

【0044】また、以上の実施形態におけるICカードリーダライタを、単に、アクセスキーの読み書きを行う

装置とし、ICカードリーダライタを介して、PC103が、先に図4に示した処理を行うようにしてもよい。

【0045】また、図5のステップ505では、入力された認証データとアクセスキー101に記憶されている認証データを比較するようにしてもよい。

【0046】また、以上の実施形態では、各アクセスキーの使用可能／不可を表す使用可能／不可判別用データを、個々のアクセスキーに記憶して使用したが、全てのアクセスキーについての使用可能／不可判別用データをPC103側に記憶し、使用するようにしてもよい。ただし、この場合において、アクセスキーが複数のPC103で使用されるものである場合には、PC103間で全てのアクセスキーについての使用可能／不可判別用データを交換し、各アクセスキーの使用可能／不可判別用データを最新の状態に維持するようにする。

【0047】

【発明の効果】以上のように、本発明によれば、システム利用途中でアクセスキーをシステムに接続したまま、利用者がシステムを離れてしまった場合に、第三者による、システムへの不正なアクセスを排除することができる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る電子計算機システムの構成を示すブロック図である。

【図2】本発明の実施形態に係る電子計算機システムのソフトウェア構成を示すブロック図である。

【図3】本発明の実施形態に係る電子計算機のハードウェア構成を示すブロック図である。

【図4】本発明の実施形態に係る認識監視処理プログラムの動作の手順を示すフローチャートである。

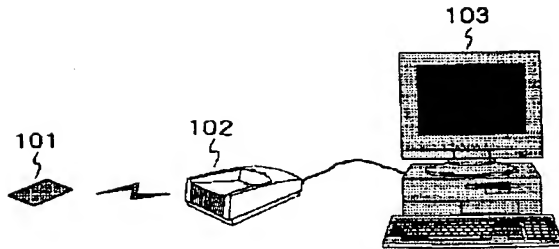
【図5】本発明の実施形態に係るアクセスキー処理プログラムの動作の手順を示すフローチャートである。

【符号の説明】

101 アクセスキー
102 ICカードリーダライタ
103 PC
203 認識監視処理プログラム
205 アクセスキー処理プログラム

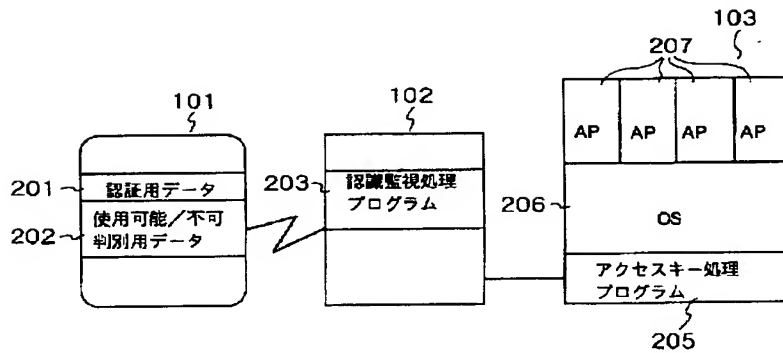
【図1】

図1



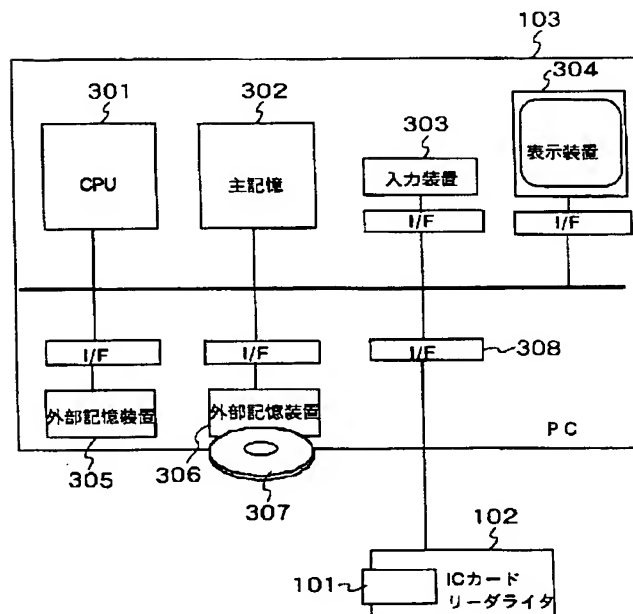
【図2】

図2



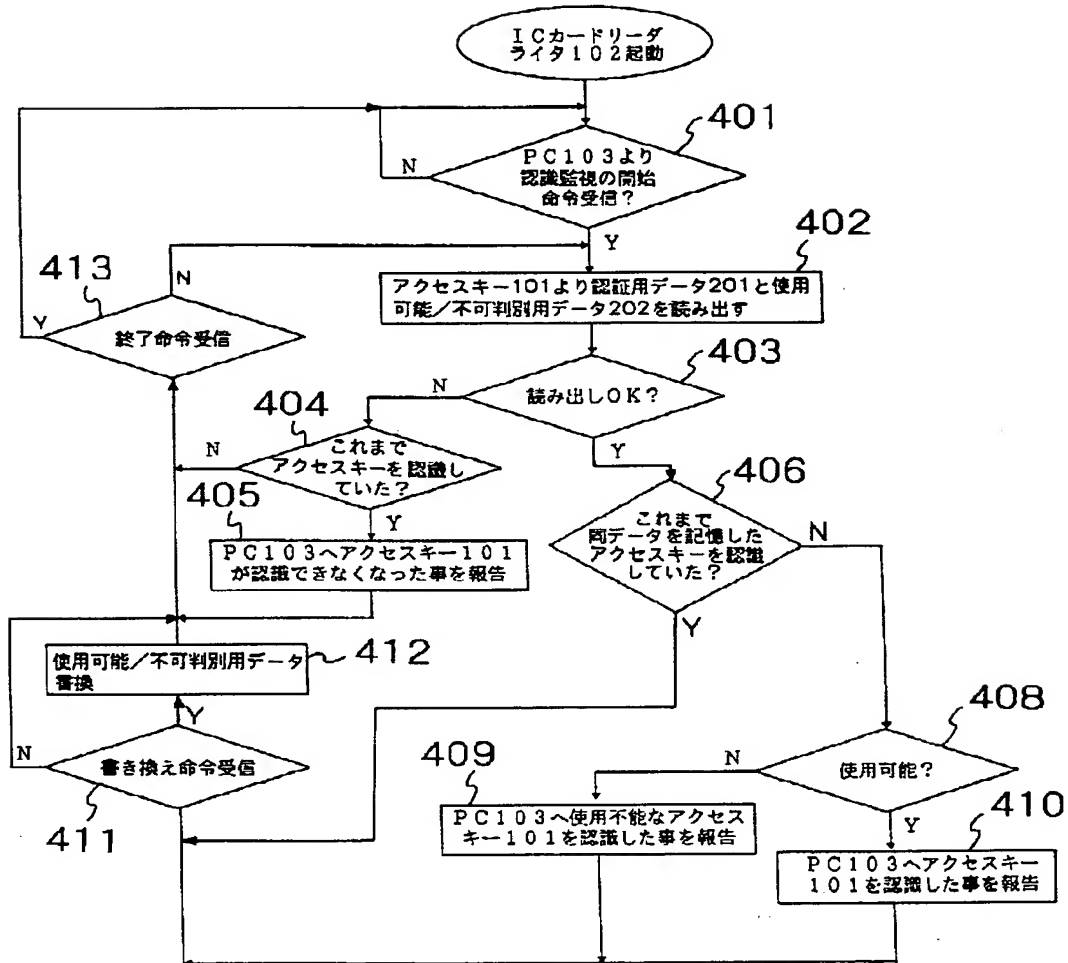
【図3】

図3



【図4】

図4



【図5】

図5

